Article

Sensor Network Security and Risk Assessment

Yaswanth Chandolu and Ehsan Sheybani *

Posted Date: 18 October 2023

doi: 10.20944/preprints202310.1106.v1

Keywords: sensor networks; risk; security; vulnerability

Article

Sensor Network Security and Risk Assessment

Yaswanth Chandolu and Ehsan Sheybani *

Business Analytics and Information Systems, University of South Florida; yaswanth2@usf.edu
* Correspondence: sheybani@usf.edu

Abstract: in our increasingly interconnected world, sensor networks are critical in gathering and sending data for various applications, from environmental monitoring and industrial automation to healthcare and smart cities. However, as sensor networks expand in importance, so does the need to solve the multidimensional concerns of security, privacy, and forensics. This article explores the complex world of sensor network security, the delicate balance between data privacy and utility, and the emerging area of sensor network forensics. This article focuses on risk assessment of a network.

Keywords: sensor networks; risk; security; vulnerability

1. Introduction

The increasing dependence on computer networks for communication and data exchange has made them an attractive target for attackers. Network devices such as routers, switches, firewalls, and servers are critical components of a network and are the primary targets of attackers. These devices are vulnerable to various types of attacks, including malware, denial-of-service (DoS) attacks, and hacking attempts. This article aims to provide detailed information about procedures to identify the sources of risk associated with network devices and the parameters that affect risk the most. It will also provide a methodology to assign a risk score to a network based on the identified parameters.

1.1. Sources of Risk of Network Devices:

The following are the primary sources of risk associated with network devices:

Software Vulnerabilities: Network devices run on software, and any software can have vulnerabilities that attackers can exploit. A vulnerability is a weakness in the software that an attacker can use to gain unauthorized access or control of the device.

Misconfiguration: Misconfiguration occurs when network devices are not set up correctly, leading to security holes that attackers can exploit. Misconfiguration can also result in poor performance or even network downtime.

Insider Threats: Insider threats refer to the risk of an attack or data breach by an employee or someone with authorized access to the network. Insider threats can be intentional, such as a disgruntled employee seeking revenge, or unintentional, such as an employee accidentally exposing sensitive information.

Social Engineering: Social engineering is a technique used by attackers to manipulate people into divulging sensitive information or performing actions that compromise network security. Social engineering attacks can take many forms, including phishing, pretexting, and baiting.

Physical Threats: Physical threats refer to the risk of damage or theft of network devices. An attacker can gain physical access to a device and tamper with it, steal it, or destroy it.

1.2. Parameters Affecting Risk:

The following parameters have the most significant impact on the risk associated with network devices:

Network Complexity: The complexity of a network is a crucial factor in its risk management. A complex network is more challenging to manage and secure than a simple network, making it more vulnerable to attacks.

Access Control: Access control refers to the process of granting or denying access to network resources. Weak access control mechanisms can lead to unauthorized access, increasing the risk of attacks.

Patch Management: Patch management is the process of applying updates to software and devices to address security vulnerabilities. Poor patch management practices can leave network devices vulnerable to known exploits.

Security Monitoring: Security monitoring involves the continuous monitoring of network devices to detect and respond to security incidents. Inadequate security monitoring can delay detection and response to attacks, increasing the risk of damage.

Employee Training: Employee training refers to the process of educating employees on network security best practices and procedures. A lack of employee training can lead to unintentional security breaches, increasing the risk of attacks.

2. Vulnerability scanning

Vulnerability scanning is the process of identifying potential security vulnerabilities in a network, system, or application In the ever-evolving landscape of cybersecurity, vulnerability scanning stands as a critical defense mechanism against potential threats lurking within digital ecosystems. This proactive approach involves the systematic exploration of computer systems, networks, and applications to identify vulnerabilities that could be exploited by malicious actors. Vulnerability scanning not only serves as an initial line of defense but also provides organizations with valuable insights into their digital infrastructure's weaknesses. By shining a light on these vulnerabilities, organizations can take targeted measures to fortify their defenses and enhance their overall security posture. In an era where digital assets are constantly under siege, vulnerability scanning emerges as an indispensable practice to safeguard sensitive information and maintain the integrity of digital operations.

In an interconnected world teeming with sophisticated cyber threats, the importance of vulnerability scanning cannot be overstated. As organizations increasingly rely on digital technologies to streamline operations, deliver services, and store sensitive data, they also become more susceptible to cyberattacks. Vulnerability scanning acts as a proactive shield, enabling organizations to identify and rectify potential weak points before malicious actors capitalize on them. By regularly assessing systems and applications for vulnerabilities, organizations can effectively reduce the attack surface, thwart potential breaches, and adhere to regulatory compliance standards. In this dynamic cybersecurity landscape, vulnerability scanning empowers organizations to stay one step ahead of cyber threats and maintain the trust of their stakeholders. There are several methods for vulnerability scanning, including:

Network Scanning: Network scanning involves using automated tools to scan a network for vulnerabilities. The tools scan open ports, network services, and protocols to identify potential vulnerabilities.

Host-based Scanning: Host-based scanning involves scanning individual devices, such as servers, desktops, or laptops, to identify vulnerabilities in the operating system, installed applications, and system configurations.

Application Scanning: Application scanning involves scanning web applications and databases to identify potential vulnerabilities. The tools simulate attacks and analyze the application's response to identify vulnerabilities, such as SQL injection or cross-site scripting.

Manual Testing: Manual testing involves testing the network, system, or application manually to identify vulnerabilities. Manual testing requires expertise and may be time-consuming, but it can provide a more comprehensive assessment of the security posture.

Cloud-Based Scanning: Cloud-based scanning involves scanning cloud-based infrastructure and applications for vulnerabilities. The tools are designed to scan the cloud environment, including virtual machines, storage, and databases.

Passive Scanning: Passive scanning involves monitoring network traffic to identify potential vulnerabilities. Passive scanning does not generate traffic, making it less intrusive and suitable for environments with strict security requirements.

Vulnerability scanning is a crucial part of network security management. Organizations should perform regular vulnerability scanning to identify potential threats and vulnerabilities and take appropriate measures to mitigate them.

2.1. Tools for Vulnerability Scanning

There are various tools available that can be used to perform vulnerability scans. In this report, we will discuss some of the most popular vulnerability scanning tools.

Nessus:

Nessus is one of the most widely used vulnerability scanning tools. It provides comprehensive vulnerability scanning for networks, operating systems, and applications. Nessus can detect vulnerabilities in operating systems, web applications, databases, and more. It also includes pre-built compliance templates to check if systems are meeting security standards. Nessus can be run on a variety of operating systems, including Windows, Linux, and macOS.

OpenVAS:

OpenVAS is an open-source vulnerability scanning tool that provides a comprehensive vulnerability scanning solution. OpenVAS can detect vulnerabilities in operating systems, network services, and applications. It also provides a web-based interface for managing and running scans. OpenVAS is compatible with Linux, Windows, and macOS.

Qualys:

Qualys is a cloud-based vulnerability scanning tool that provides continuous monitoring of IT infrastructure. It can detect vulnerabilities in web applications, operating systems, and network devices. Qualys provides real-time reports and alerts for vulnerabilities and can also provide remediation guidance. Qualys is compatible with a variety of operating systems and platforms, including Windows, Linux, macOS, and cloud environments.

Acunetix:

Acunetix is a web application vulnerability scanning tool that can detect SQL injection, cross-site scripting (XSS), and other vulnerabilities in web applications. It provides a comprehensive set of tools for web application scanning, including a vulnerability scanner, HTTP editor, and site crawler. Acunetix can be run on a variety of operating systems, including Windows, Linux, and macOS.

Nikto:

Nikto is an open-source web server scanner that can detect vulnerabilities in web servers, web applications, and scripts. It can detect vulnerabilities such as outdated software versions, default files and directories, and misconfigured servers. Nikto is compatible with Linux, Windows, and macOS.

Metasploit:

Metasploit is a penetration testing framework that can be used to identify and exploit vulnerabilities in computer systems, networks, and applications. It provides a comprehensive set of tools for penetration testing, including exploit modules, payloads, and auxiliary modules. Metasploit is compatible with Linux, Windows, and macOS.

In conclusion, there are several tools available for vulnerability scanning, each with its strengths and weaknesses. The selection of a vulnerability scanning tool should be based on the specific requirements and needs of an organization. It is also recommended to use a combination of tools to provide comprehensive coverage for vulnerability scanning.

2.2. Tools for Network Risk-Scoring

To effectively safeguard digital ecosystems, organizations rely on a suite of advanced tools specifically designed for the evaluation of network-related risks. These tools serve as vigilant sentinels, tirelessly scouring network landscapes for vulnerabilities, analyzing potential consequences, and empowering organizations to make informed decisions that bolster their cyber defenses. we delve into the array of tools available for evaluating network risks, shedding light on their capabilities and contributions to the overarching goal of fortifying digital resilience.

Network risk scoring tools are used to assess the level of risk to a network or system. These tools assign scores to various aspects of the network, such as vulnerabilities, threats, and assets, to determine the overall risk level. In this report, we will discuss some of the most popular network risk-scoring tools.

2.2.1. Common Vulnerability Scoring System (CVSS):

The Common Vulnerability Scoring System (CVSS) is a widely used tool for assessing the severity of vulnerabilities in computer systems. It assigns scores to vulnerabilities based on their impact, exploitability, and other factors. The scores range from 0 to 10, with higher scores indicating higher levels of risk.

The methodology behind scoring:

The CVSS methodology consists of three main components: the Base Score, the Temporal Score, and the Environmental Score. Each of these components provides a different perspective on the vulnerability and its potential impact.

2.2.1.1. Base Score:

The Base Score is the fundamental component of the CVSS methodology. It is used to evaluate the intrinsic characteristics of the vulnerability, such as the type of vulnerability, the potential impact on the system, and the level of exploitability. The Base Score consists of three metric groups:

Exploitability Metrics: These metrics evaluate the ease of exploiting the vulnerability, such as the complexity of the attack and the level of user interaction required. The Exploitability Metrics are scored on a scale of 0 to 10, with higher scores indicating easier exploitability.

There are five exploitability metrics that are used to calculate the Base Score: Attack Vector, Attack Complexity, Privileges Required, User Interaction, and Scope.

Attack Vector:

The Attack Vector metric describes how an attacker can exploit the vulnerability to gain access to the system. There are four possible values for this metric:

Network: the vulnerability can be exploited over the network, without any interaction from the user

Security Requirements: This metric evaluates the impact of any security requirements that may mitigate vulnerability.

The Security Requirements (SR) metric is one of the metrics used to calculate the Temporal score of the Common Vulnerability Scoring System (CVSS). This metric measures the level of security requirements that must be satisfied to exploit the vulnerability.

The SR metric has the following possible values:

Not Defined (X): There is no information available about the security requirements for the vulnerability.

Low (L): The vulnerability can be exploited with little to no special access or privileges.

Medium (M): The vulnerability can be exploited with some level of access or privileges, but not all.

High (H): The vulnerability can only be exploited with full access or privileges.

The logic behind the evaluation of the SR metric is as follows:

If there is no information available about the security requirements for the vulnerability, the value for SR is X.

If the vulnerability can be exploited with little to no special access or privileges, the value for SR is L.

If the vulnerability can be exploited with some level of access or privileges, but not all, the value for SR is M.

If the vulnerability can only be exploited with full access or privileges, the value for SR is H.

The higher the value of SR, the greater the level of security requirements that must be satisfied to exploit the vulnerability. Therefore, vulnerabilities with a higher SR value will have a lower Temporal score than vulnerabilities with a lower SR value.

It is important to note that the SR metric only measures the level of security requirements at the time of evaluation. As new security requirements are identified, the SR metric may change, and the Temporal score may be recalculated.

The Temporal Score is calculated by combining the scores from each of the four metric groups. The resulting score is then added to the Base Score to provide an overall score for the vulnerability.

2.2.1.2. Environmental Score:

The Environmental Score is used to evaluate the impact of the vulnerability on a specific environment, such as a particular network or system. The Environmental Score consists of three metric groups:

Collateral Damage Potential: This metric evaluates the potential impact on other systems or resources in the environment.

Target Distribution: This metric evaluates the number of targets in the environment that are vulnerable to exploitation.

Confidentiality Requirement: This metric evaluates the level of confidentiality required in the environment.

The Environmental Score is calculated by combining the scores from each of the three metric groups. The resulting score is then added to the Base Score to provide an overall score for the vulnerability in the specific environment.

In conclusion, the Common Vulnerability Scoring System (CVSS) provides a comprehensive methodology for assessing the severity of vulnerabilities in computer systems. The methodology consists of three main components: the Base Score, the Temporal Score, and the Environmental Score. By using this methodology, organizations can accurately and consistently assess the risk posed by vulnerabilities and prioritize their response accordingly.

3. Drawbacks in Network Risk Evaluation Scoring Tools

While network risk evaluation scoring tools play a crucial role in identifying and prioritizing vulnerabilities, it is essential to recognize that no solution is without its limitations. These tools, designed to streamline the assessment of network risks, come with their own set of drawbacks that merit careful consideration. As organizations navigate the complex landscape of cybersecurity, it is imperative to comprehend these limitations to make informed decisions about the implementation and utilization of such tools. In this section, we explore the potential drawbacks inherent in network risk evaluation scoring tools, shedding light on areas that require nuanced understanding and supplementary strategies for a comprehensive defense posture.

Limited focus: CVSS only assesses the technical aspects of a vulnerability and does not consider other important factors such as business impact, compliance requirements, or the likelihood of exploitation. This narrow focus may result in an incomplete or inaccurate risk assessment.

Limited accuracy: CVSS scores are based on a predefined set of metrics, which may not always accurately reflect the real-world impact of a vulnerability. For example, a vulnerability with a high CVSS score may not necessarily be the most critical issue for an organization, while a vulnerability with a low score may still pose a significant risk.

Complexity: The CVSS scoring system can be complex and difficult to understand, especially for non-technical stakeholders. This may lead to confusion or misinterpretation of the results, which could in turn impact decision-making.

Over-reliance: There is a risk of over-reliance on CVSS scores to prioritize vulnerability remediation efforts. Organizations may focus only on vulnerabilities with the highest scores, while neglecting other important factors such as business criticality or ease of exploitation.

Lack of context: CVSS scores do not provide context on the specific environment or configuration of the affected system, which can be important in determining the actual risk posed by a vulnerability.

4. Using Machine Learning in Risk Evaluation of Networks

Explanation with real-time example

Let's consider a hypothetical example of an organization that has recently experienced a data breach. Using a traditional risk evaluation method, the organization might assign a score to the breach based on factors such as the type of data that was exposed, the number of records that were compromised, and the likelihood of a similar breach occurring in the future.

However, this traditional approach may fail to capture the full complexity of the situation. For example, the scoring system may not consider the sophistication of the attacker, the specific vulnerabilities that were exploited, or the effectiveness of the organization's security controls in detecting and responding to the breach.

In contrast, a machine learning model could provide a more accurate assessment of the risk associated with the breach. By analyzing historical data on cyber-attacks and vulnerabilities, the model could identify patterns and trends that might not be immediately apparent using traditional scoring systems. The model could consider factors such as the attacker's tactics, techniques, and procedures (TTPs), the vulnerabilities that were exploited, and the effectiveness of the organization's security controls in detecting and responding to the breach.

Using this information, the machine learning model could provide a more accurate assessment of the risk associated with the breach and recommendations for improving the organization's vulnerability management practices. For example, the model might suggest specific security controls or remediation strategies based on the characteristics of the breach or provide guidance on how to prioritize vulnerabilities based on their potential impact.

Overall, this example illustrates how traditional risk evaluation methods can produce inaccurate results compared to machine learning models. While traditional methods may be useful for certain types of assessments, they often fail to capture the full complexity of real-world cyber risk and may not be able to keep up with the rapidly changing threat landscape. By leveraging the power of machine learning algorithms, organizations can gain deeper insights into their cyber risk posture and make more informed decisions about how to allocate resources for mitigating cyber risk.

The Cyentia Institute's Risk Insights project is a research effort that uses machine learning algorithms to analyze historical data on cyber risk and vulnerability management. The project aims to identify trends and patterns in vulnerability data that can be used to improve risk assessment and decision-making.

The project involves several stages of data analysis and modeling. First, the project team collects and cleanses a large dataset of vulnerability data, including information on the severity, type, and potential impact of each vulnerability. The dataset also includes contextual information such as the affected system or application, the industry vertical, and the presence of security controls.

Next, the team uses machine learning algorithms to identify patterns and trends in the vulnerability data. This involves applying clustering algorithms to group similar vulnerabilities together, and classification algorithms to identify the characteristics of high-risk vulnerabilities.

Once the machine learning models have been trained, the project team can use them to generate predictive analytics on future attack trends. For example, the team might use the models to predict which vulnerabilities are most likely to be exploited in the next 12 months, or to identify emerging attack vectors that are not currently well-understood.

Finally, the project team uses the insights generated from the machine learning models to develop best practices and recommendations for vulnerability management. This might involve recommending specific security controls or remediation strategies based on the characteristics of a particular vulnerability or providing guidance on how to prioritize vulnerabilities based on their potential impact.

Overall, the Cyentia Institute's Risk Insights project is an innovative approach to vulnerability risk assessment that leverages the power of machine learning to identify patterns and trends in vulnerability data that might not be immediately apparent using traditional scoring systems. The project has the potential to significantly improve the accuracy and effectiveness of vulnerability management practices in a wide range of industries and settings.

5. Challenges of Using Machine Learning in Risk Evaluation

While machine learning can be a powerful tool for risk evaluation, there are several challenges that must be addressed to ensure its effectiveness and accuracy. Some of the key challenges of using machine learning in risk evaluation are:

Data Quality: Machine learning models are only as good as the data they are trained on. Poor quality or incomplete data can lead to inaccurate or biased predictions. Therefore, it is crucial to ensure that the data used to train machine learning models is of high quality and accurately represents the target population.

Data Bias: Machine learning models can be biased towards certain groups or outcomes if the training data is not representative. This can lead to inaccurate or unfair predictions, particularly in areas such as lending or hiring where bias can have significant real-world consequences. It is therefore important to carefully select and preprocess the data to minimize bias in the model.

Model Interpretability: Machine learning models can be difficult to interpret, particularly when using complex algorithms such as neural networks or deep learning. This can make it difficult to understand how the model arrived at its predictions and to identify potential biases or errors. Therefore, it is important to ensure that machine learning models are designed with interpretability in mind, and that model outputs can be easily explained and validated.

Overfitting: Machine learning models can also suffer from overfitting, where the model is too closely tailored to the training data and does not generalize well to new data. This can lead to poor performance and inaccurate predictions. Therefore, it is important to carefully select the model architecture and regularization techniques to prevent overfitting.

Cost and Resources: Machine learning models can be computationally expensive and require large amounts of data and computational resources. This can make it difficult for small businesses or organizations with limited resources to implement machine learning-based risk evaluation systems. Therefore, it is important to carefully balance the computational requirements of the model with the available resources and expertise.

In conclusion, while machine learning can be a powerful tool for risk evaluation, there are several challenges that must be addressed to ensure its effectiveness and accuracy. These challenges include data quality, data bias, model interpretability, overfitting, and cost and resources. By carefully considering these challenges and addressing them appropriately, machine learning can be used to develop accurate and effective risk evaluation systems.

6. Results

The investigation into the evaluation of risk associated with network vulnerabilities unveiled a comprehensive landscape of tools, each offering distinct methodologies for identifying and prioritizing potential threats. Our analysis encompassed a spectrum of approaches, ranging from manual assessment and qualitative scoring systems to advanced automated tools. Notably, machine learning algorithms emerged as the standout solution, exhibiting unparalleled efficacy in enhancing risk evaluation accuracy and efficiency.

Comparison across the examined tools highlighted the limitations of traditional manual methods, which often struggled to keep pace with the ever-evolving threat landscape and the growing complexity of network architectures. While qualitative scoring systems provided valuable insights, they were constrained by subjectivity and lacked the precision demanded for a robust risk assessment.

In contrast, machine learning algorithms showcased their prowess in mitigating these limitations. By ingesting vast datasets and learning intricate patterns, these algorithms demonstrated a remarkable ability to discern hidden correlations, enabling more accurate risk prediction. The integration of machine learning techniques empowered organizations to swiftly process enormous amounts of data, identify emerging threats, and adapt risk evaluation strategies in real-time.

7. Conclusion

In the quest for an effective approach to evaluating network risk, this study has underscored the transformative potential of machine learning algorithms. Traditional methodologies, while valuable, fall short in today's dynamic cybersecurity landscape, where agility and precision are paramount. Machine learning algorithms stand as the vanguard of risk evaluation, harnessing the power of data-driven insights to fortify digital defenses.

The journey from manual assessments to sophisticated machine learning models signifies a paradigm shift in network risk evaluation. As organizations strive to safeguard their digital assets and maintain operational continuity, the integration of machine learning algorithms emerges as the strategic imperative. By adopting these advanced tools, organizations can proactively identify vulnerabilities, predict potential threats, and deploy targeted countermeasures, thereby enhancing their cyber resilience and establishing a robust defense against ever-evolving risks. It is evident that machine learning algorithms have revolutionized the landscape of network risk evaluation, representing a formidable leap towards a more secure digital future.

Acknowledgments: This research is funded by the Research Office at the University of South Florida, Sarasota-Manatee Campus, from the IRG Interdisciplinary Research Grant awarded to Dr. Sheybani.

References

1. Süzen, A. A. (2020). A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem. *International Journal of Computer Network & Information Security*, *12*(1).
2. Sebastian, D. J., & Hahn, A. (2017, September). Exploring emerging cybersecurity risks from network-connected DER devices. In *2017 North American Power Symposium (NAPS)* (pp. 1-6). IEEE. Oser, P., Engelmann, F., Lüders, S., & Kargl, F. (2023, April).
3. Evaluating the Future Device Security Risk Indicator for Hundreds of IoT Devices. In *Security and Trust Management: 18th International Workshop, STM 2022, Copenhagen, Denmark, September 29, 2022, Proceedings* (pp. 52-70). Cham: Springer International Publishing.
4. Daud, N. I., Bakar, K. A. A., & Hasan, M. S. M. (2014, August). A case study on web application vulnerability scanning tools. In *2014 Science and Information Conference* (pp. 595-600). IEEE.
5. Daud, N. I., Bakar, K. A. A., & Hasan, M. S. M. (2014, August). A case study on web application vulnerability scanning tools. In *2014 Science and Information Conference* (pp. 595-600). IEEE.
6. Holm, H. (2012). Performance of automated network vulnerability scanning at remediating security issues. *Computers & Security*, *31*(2), 164-175.
7. Wang, Y., Bai, Y., Li, L., Chen, X., & Chen, A. (2020, June). Design of network vulnerability scanning system based on NVTs. In *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)* (pp. 1774-1777). IEEE.
8. Paltrinieri, N., Comfort, L., & Reniers, G. (2019). Learning about risk: Machine learning for risk assessment. *Safety science*, *118*, 475-486.
9. Hegde, J., & Rokseth, B. (2020). Applications of machine learning methods for engineering risk assessment–A review. *Safety science*, *122*, 104492.
10. Angelini, E., Di Tollo, G., & Roli, A. (2008). A neural network approach for credit risk evaluation. *The quarterly review of economics and finance*, *48*(4), 733-755.
11. Mell, P., Scarfone, K., & Romanosky, S. (2006). Common vulnerability scoring system. *IEEE Security & Privacy*, *4*(6), 85-89.
12. E. Doynikova, A. Chechulin and I. Kotenko, "Analytical attack modeling and security assessment based on the common vulnerability scoring system," 2017 20th Conference of Open Innovations Association (FRUCT), St. Petersburg, Russia, 2017, pp. 53-61, doi: 10.23919/FRUCT.2017.8071292.

13. Bolívar, H., Parada, H. D. J., Roa, O., & Velandia, J. (2019, October). Multi-criteria decision making model for vulnerabilities assessment in cloud computing regarding common vulnerability scoring system. In *2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI)* (pp. 1-6). IEEE.
14. Ou, X., Singhal, A., Ou, X., & Singhal, A. (2011). The common vulnerability scoring system (CVSS). *Quantitative Security Risk Assessment of Enterprise Networks*, 9-12.
15. Y. Yamamoto, D. Miyamoto and M. Nakayama, "Text-Mining Approach for Estimating Vulnerability Score," 2015 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), Kyoto, Japan, 2015, pp. 67-73, doi: 10.1109/BADGERS.2015.018.
16. Paltrinieri, N., Comfort, L., & Reniers, G. (2019). Learning about risk: Machine learning for risk assessment. *Safety science*, *118*, 475-486.
17. A. Singh, N. Thakur and A. Sharma, "A review of supervised machine learning algorithms," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016, pp. 1310-1315.
18. Attaran, M., & Deb, P. (2018). Machine learning: the new'big thing'for competitive advantage. *International Journal of Knowledge Engineering and Data Mining*, *5*(4), 277-305.
19. Mazhar, T., Irfan, H. M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). Analysis of Cyber Security Attacks and Its Solutions for the Smart Grid Using Machine Learning and Blockchain Methods. *Future Internet*, *15*(2), 83
20. Chen, Q., Chen, Z., Nafa, Y., Duan, T., Pan, W., Zhang, L., & Li, Z. (2023). Adaptive deep learning for entity resolution by risk analysis. *Knowledge-Based Systems*, *260*, 110118.
21. F. Li, "Network Security Evaluation and Optimal Active Defense based on Attack and Defense Game Model," 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballar, India, 2023, pp. 1-7, doi: 10.1109/ICDCECE57866.2023.10151226.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.